- Title **Requirements to Use or Disclose Protected Health Information**

- Creation
  - Date 1-16-01
  - Author Ginger Cox
  - Phone number 916-327-2249
  - Email address (www.dds.ca.gov/HipaaSecurity)

- Revision
  - Date 5-11-01
  - Author Ginger Cox
  - Phone number 916-327-2249
  - Email address gcox@oshpd.state.ca.us

I. Introduction

This template is designed to help any government entities who are required or who desire to protect individually identifiable health information, in electronic and non-electronic forms, including paper records and oral communication.

II. Purpose

The purpose is to comply with the requirements of a national framework for health information privacy protection. This is necessary to ensure the patient's right to privacy, to protect and enhance the patient's rights to access health information, and to control inappropriate use of that information.

A. Specific national HIPAA requirements/standards addressed

The requirements are to comply with the general administrative requirements and with the standards to privacy of individually identifiable health information. (45 Code of Federal Regulations, Parts 160, 164 of the HIPAA)

B. Areas in which this template should be utilized

This template addresses:
- what is protected health information,
- who can or cannot use or disclose this information,
- how much of the information can be released,
- whether preemption of state law applies or does not apply, and
- acknowledgement of violation penalties.

This template does not address:

- fee assessments for data release,
- request forms, consent forms, authorization forms, entity's approval forms,
- user access procedures,
- security control mechanisms, or
- system operations for receiving, maintaining, and retaining the protected health information.

C. Pertinent References

The pertinent reference is: Federal Register dated 12/28/00, 45 Code of Federal Regulations, Parts 160 and 164, on Standards for Privacy of Individually Identifiable Health Information. The final Privacy Rule complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) standard for privacy of individually identifiable health information. For all covered entities, the required date of compliance is 4/14/03, with the following exception. A small health plan with annual receipts of $5 million or less, has a required date of compliance of 4/14/04.

III. Assumptions

Any requests for protected health information to the entity, whether internal or external, are now subject to review prior to release.

The potential for misuse or unauthorized release of protected health information exists every time someone accesses or releases such information. Lack of training or knowledge regarding protected health information affects the covered entity's ability to comply with use and disclosure requirements of HIPAA.

Every paper, fax, computer printout, computer screen, e-mail, laptop, back-up system, or oral communication containing protected health information is vulnerable to unauthorized access, whether unintentional or intentional.

No computer user within the entity may access, save, manipulate, or destroy protected health information without proper authorization.

IV. Pre-requisites

Adherence to entity's security policy and procedures.
Adherence to entity's policy on use of protected health information (e-mail, fax, paper, computer, oral, online transmission, and media).
Adherence to Confidentiality Statements.
Adherence to Business Associate Agreement when applicable.
Adherence to state laws such as FOIA, ERISA, CLIA, ADA, Safe Harbor, FDA regulations, Information Practices Act, and the PHS act, except where such laws are preempted by HIPAA.
Adherence to agency specific codes, rules, and regulations unless preempted by HIPAA.

V. Constraints

Timeliness for release of protected health information is critical.
Different types of requests for protected health information should have specific priorities and release timeframes assigned.

V1. Dependencies

All members of the workforce, as well as its business associate(s) and subcontractors are responsible for implementing the entity's policy and procedures regarding the release of protected health information.

VII. Process

The process includes the written policy and procedures set out by the entity regarding proper release and disclosure of protected health information, in response to internal and/or external requests.

VIII. Procedures

A. Preventive measures

Provide training to all members of its workforce, including business associates, regarding entity's policy and procedures for consistent business practices in receiving, maintaining, handling, accessing, manipulating, releasing, retaining, and destroying protected health information. (Section 164.530).

Develop policies to address fax, e-mail, oral communication, or computer on-line transmission of protected health information. (Sections 160.102, 164.502, and 164.522).

Ensure that no employee(s) may access any protected health information that the employee(s) does not have a business need to know. (Section 164.530).

Ensure that no employee(s) may disclose protected health information unless properly authorized. See entity's policy and procedures for disclosures and penalties. (Section 164.530).

B. Guidelines

1. Provide clear definitions of protected health information, disclosures, and uses:

    a) Protected health information means individually identifiable health information transmitted or maintained in any form or medium.

b) Individually identifiable health information is a subset of protected health information, including demographic information:

- collected from an individual;
- created or received by a health care provider, health plan, employer, or health care clearinghouse;
- relates to the past, present, or future physical or mental health or condition of an individual;
- relates to the provision of health care to an individual;
- relates to the past, present, or future payment for the provision of health care to an individual;
- identifies an individual, where there is a reasonable basis to believe the information can be used to identify the individual. (Section 164.501)

c) Disclosure means the release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to the entity holding the information. (Section 164.501)

d) Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (Section 164.501)

2. Covered Entities' Requirements in Protected Health Information

The HIPAA regulation for covered entities applies only to health plans, health care clearinghouses, and health care providers who handle individually identifiable health information. In hybrid entities, only the subsidiary or subdivision that performs covered functions is bound by the regulation. (Sections 160.102, 164.104, 164.106)

Only information created or collected by these covered entities is protected by the HIPAA regulation. Individually identifiable health information that is collected from any other legitimate source (such as employers and educational facilities when not acting as providers or plans) can be fully used without utilizing the procedures required by the regulation. (Sections 164.501)

The covered entity must ensure, through contract or other written agreement, that business associate(s) who receive protected health information from the covered entity only use or disclose the information for the specific purposes they were given the information. (Sections 160.103, 164.502(e), 164.504(e))

Depending on the entity and its relationship with another entity or person(s), consents or authorizations may be required. (Section 164.501, 164.506)

The covered entity must:

- designate a Privacy Official;
- provide notice of privacy practices for protected health information;
- train all members of its workforce on policy and procedures with respect to protected health information;
- comply with administrative, technical, and physical safeguards in protecting the privacy of health information;
- identify staff requiring access to protected health information and define the level of access;
- monitor protected health information from inappropriate use or disclosure that is in violation of the privacy rule; and
- implement the policies and procedures related to protected health information. (Section 164.520, 164.530)

3. Business Associates' Requirements regarding Protected Health Information

Any entity that creates or receives protected health information on behalf of the covered entity must adhere to the contract or other written agreement which must restrict their use of the information to the purposes described. (Sections 164.103, 164.502(e), 164.504(e))

4. Minimum Necessary Disclosure

Covered entities must make a reasonable effort to limit use and disclosure of protected health information to the minimum necessary to accomplish the intended purpose. (Section 164.502). Criteria should be developed to limit the protected health information disclosed to that information reasonably necessary to accomplish the intended purpose. (Section 164.514(d)). Requests for disclosure should be reviewed on an individual basis. (Section 164.514(d)).

Exception: The minimum necessary disclosure does not apply to a health care provider for treatment of that individual, uses or disclosures to the individual who is subject of protected health information, uses or disclosures as specified in the individual's authorization, and uses or disclosures that are required by law (Section 164.502 (b)(2)).

5. Consents

Covered entities must obtain the individual's signed consent prior to using or disclosing protected health information. A consent must be in plain language which informs the individual that protected health information may be used and disclosed to carry out treatment, payment or health care operations. (Section 164.506).

Exception: Psychotherapy notes are in a more stringent category of protected health information. Authorization from the patient is always necessary before these notes may be used or disclosed. (Section 164.501)

6. Authorizations

   An authorization is more detailed than the consent. A covered entity must obtain the individual's signed authorization prior to using or disclosing protected health information. The authorization must be in plain language that includes information to be disclosed, recipient of information, expiration date, and a statement of individual's right to revoke the authorization. (Section 164.508)

7. Permitted Uses and Disclosures

   - To the individual who is the subject of the protected health information (Section 164.501 and 164.502), or
   - To the provider to carry out treatment of that patient (Section 164.502), or
   - Under a signed consent (Section 164.502), or
   - Where consent is not required (Section 164.506(a)), or
   - With valid authorization (Section 164.508), or
   - With individual's oral agreement (Section 164.510), or
   - By a whistleblower or workforce member or business associate to Office of Civil Rights as a health oversight agency, law enforcement official, or attorney in investigation for violation of protected health information standards (Section 164.502(j)).

8. Required Disclosures

   - To the individual who is the subject of the protected health information (Sections 164.501, 164.502 164.524, 164.528), or
   - As required by law (Section 164.512), or
   - To public health activities (Section 164.512), or
   - To workers' compensation carriers (Section 164.512), or
   - To health oversight activities (Section 164.512), or
   - To law enforcement and for use in any judicial and administrative proceedings subject to warrant and/or subpoena (Section 164.512), or
   - For research purposes with Institutional Review Board's approval or a qualified privacy board's approval (Section 164.512), or
   - To the Secretary/Office of Civil Rights for investigative issues concerning privacy rule compliance (Section 164.512).

9. Uses or Disclosures Not Allowed

   - Marketing purposes in product or service without the individual's signed authorization, except for the covered entity's marketing communication (Sections 164.501 and 164.514(e)), or
   - Fundraising purposes, unless a statement is included in the covered entity's notice (Section 164.514(f)), or
   - Health plan's underwriting and related purposes, except as may be required by law (Section 164.514(g)).

10. Uses and Disclosures for Research Purposes

A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that an Institutional Review Board's approval of the waiver of authorization in accordance with Code of Federal Regulations is obtained. (Section 164.512(i)).

In the absence of an Institutional Review Board, a privacy board's approval of the waiver of an authorization may be obtained. The privacy board membership must consist of varied backgrounds and appropriate professional competency to review research protocol, must have at least one member who is not affiliated with either the covered entity or any entity sponsoring or conducting the research, and its members may not review projects where a conflict of interest exists. (Section 164.512(i)).

A waiver criteria from the Institutional Review Board or privacy board contains the following requirements: (Section 164.512(ii))

a) use or disclosure of protected health information presents only minimal risk to the individuals.
b) the waiver of authorization will not adversely affect the privacy rights and the welfare of the individuals.
c) research could not practicably be conducted without the waiver.
d) research could not practicably be conducted without access to and use of the protected health information.
e) privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research.
f) adequate plans are in place to protect the identifiers from improper use and disclosure.
g) adequate plans are in place to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law.
h) adequate written assurances exist that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be allowed by the regulation.
i) there is a brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board.
j) a statement is included that indicates the waiver of authorization has been reviewed and approved under either normal or expedited review procedures by an IRB following the requirements of the Common Rule or a privacy board that reviewed the proposed research at meetings where a majority of the board members were present including the non-affiliated member(s).

11. Preemption of State Law

With respect to a use or disclosure of the privacy of individually identifiable health information, if a state law (constitution, statute, regulation, rule, common law) is more stringent than the federal HIPAA standard, requirement, or implementation, the state law preempts HIPAA. (Subpart B of Part 160).

Exception: If the disclosure is: a) required by the Secretary or Office of Civil Rights in connection with determining whether a covered entity is in compliance with the federal privacy rule; or b) to the individual who is the subject of individually identifiable health information, the preemption of state law does not apply. (Section 164.202).

12. Data Aggregation

The combining of protected health information created or received by a business associate of the covered entity to permit data analyses that relate to the healthcare operations of the respective covered entities. (Section 164.501).

13. De-identified health information (Sections 164.502(d)(2) and 164.514)

Without an authorization, covered entities may use protected health information to create de-identified health information. De-identified health information is not protected health information and therefore is not subject to protected health information release, use and disclosure restrictions.

Health information may be determined to be de-identified using either of these two criteria:

a) It is determined that the risk of identifying an individual is very small, based on the application of appropriate principles and methods by a person with knowledge and experience with generally accepted statistical and scientific methods. The methods and results of the analysis to justify such determination must be documented.

or,

b) All of the 18 identifiers are removed:
1-names
2-all geographic subdivisions smaller than a state (i.e. street address, city, county, precinct, zip code and their equivalent geocodes),
(a) exception: the first three digits of a zip code, provided all the zip codes with the same three initial zip digits contain more than 20,000 people. If there are less than 20,000 people for the first three digit zip codes, the data must be displayed as 000.

3-dates relating to an individual including, but not limited to, birth date, admit date, discharge date, date of death, procedure date, service date, enrollment date, etc.

(a) Month and day cannot be displayed for those under 90 years of age. Only year can be displayed.

(b) Month and day and year cannot be displayed for those 90 years or more. Only age category can be displayed as 90 or older.

4-telephone numbers
5-fax numbers
6-electronic mail address
7-social security numbers
8-medical record numbers
9-health plan beneficiary numbers
10-account numbers
11-certificate/license numbers
12-vehicle identifiers, including license plate numbers
13-device identifiers
14-web universal resource locators (URLs)
15-internet protocol (IP) address numbers
16-biometric identifiers, including finger and voice prints
17-full face photographic images and any comparable images, and
18-any other unique identifying number, characteristic, or code.

A covered entity may create a code or other mechanism for re-identifying the information, but it is not allowed to provide that code to any other entity. (Sections 164.514(c))

If de-identified information is re-identified, such information is then treated as protected health information. (Section 164.502(d)(2)(i)).

14. Accounting of Disclosures of Protected Health Information

The covered entity must provide to the individual a written accounting of disclosures of protected health information in the six years prior to the date of individual's request. (Section 164.528(a)).

Exception: The accounting is not required for the following disclosures: to carry out treatment, payment and health care operations; for permitted/required uses and disclosures; to persons involved in the individual's care; for national security or intelligence purposes; to correctional institutions or law enforcement officials; and for the disclosures prior to the compliance date for the covered entity. (Section 164.528(a)).

IX. Accessibility of information

This template should be available to every entity that creates or receives protected health information.

X. Compliance Criteria

A covered entity must implement policies and procedures with respect to protected health information designed to comply with the HIPAA standards, implementation specifications, or other federal requirements. The policies and procedures must be reasonably designed to ensure such compliance, taking into account the size and the type of activities that relate to protected health information. This standard of implementing policies and procedures is not to be construed to permit or excuse an action that violates any other federal standard, implementation specification, or requirement. (Section 164.530(i)).

A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the federal standards, implementation specifications, and requirements. (Section 164.530(i)).

XI. Risk (if non-compliance)

Noncompliance with the federal law includes situations where protected health information is released to unauthorized recipient(s) in violation of the entity's policy and procedures, or where improper release of individually identifiable health information causes loss of employment opportunities, loss of insurance coverage, or pain of social stigma for the affected individual. Such actions are all grounds for noncompliance with the federal law and penalties will be levied. (Section 164.530(f)).

XII. Auditing Criteria

A covered entity must:

- provide records and compliance reports to the U.S. Secretary of Health and Human Services or Office of Civil Rights,
- cooperate with complaint investigations and compliance reviews, and
- permit access to all information (books, records, accounts, other sources of information, including protected health information) during normal business hours. (Section 160.310).

XIII. Template change management process (maintenance)

Privacy and security officers, Legal Counsel, and entity's administrative staff should update the template when necessary. They should distribute such changes to all members of the workforce, business partners, and other entities as applicable. In addition, they must share such changes and information with those entities who have participated in creating this template.

XIV. Approval policy

The policy for uses and disclosures of protected health information and for performing any revisions must be approved, signed, and dated by the covered entity.

XV. Disclaimer

The information in this template is for general information only. It is not intended to provide legal advice to any entity. Please consult with your Legal Counsel before taking any action based on information appearing on this template.